Privacy Protection Legislative Scenario in Select Countries: An Exploratory Study

Author Details: Dr. Madan Lal Bhasin
Professor, School of Accountancy, College of Business
Universiti Utara Malaysia (UUM), Kedah, Malaysia

Abstract:
The right of privacy is well established in international law. In fact, consumer privacy has attracted the widespread attention of regulators across the globe. Of course, privacy laws vary throughout the globe but, unfortunately, it has turned out to be the subject of legal contention between the European Union (EU) and the United States (US). Protection of personal data privacy under the law has been shaped by the interests of multiple constituencies: individuals, commercial organizations, government agencies, law enforcement, and national security services. For corporations that collect and use personal information, now ignoring privacy legislative and regulatory warning signs can prove to be a costly mistake. One of the greatest challenges faced by privacy and data protection professionals is demonstrating that their organizations have complied with the requirements of the various laws governing the handling of personal data. The freshly revised BS10012 can help organizations to meet their privacy management obligations. This is an exploratory, descriptive and qualitative study using secondary sources of data. Here, an attempt has been made to briefly acquaint the readers' with the privacy laws prevalent in select countries. It is expected that a growing number of countries will adopt privacy laws to foster e-commerce. Undoubtedly, accountability for privacy and personal data protection needs to be a joint-effort among governments, privacy commissioners, organizations and individuals themselves. Legislators all over the world have taken notice and tried to minimize invasion of privacy but without much success.
Keywords: *Privacy protection, e-business, trust seals, government regulations, select countries.*

Globalization is a noteworthy factor behind the increased attention being paid to privacy. To do business around the world, companies have had to adapt to local cultures and regulations. According to UNESCO (2012), "The right of privacy is well established in international law. Among its key characteristics is the recognition that privacy is a fundamental human right, that it is firmly established in law, and that 'Fair Information Practices' (FIP) provided a useful articulation of privacy principles in the information world." Over the last four decades, the privacy of personal data has been the subject of legislation and litigation in both the US and the EU. Protection of personal data privacy under the law has been shaped by the interests of multiple constituencies: individuals, commercial organizations, government agencies, law enforcement, and national security services (Cobb, 2016). Hence, legislators all over the world have taken notice and tried to minimize invasion of privacy. "On the surface, it seems obvious that privacy rights should be protected, but the common standard applied differs from country to country. For example, privacy laws in the European Union (henceforth, EU) are much stricter than those in the United States (henceforth, US), which implies that US companies who want to do business in the European Union must follow the EU standard," said Bhasin (2012a). Recently, Stevens (2016) pointed out that "the EU Data Protection Directive has created a legislative landscape whereby each EU Member State has implemented local data protection laws that reflect their interpretation of the Directive, their local cultural and commercial sensitivities. Germany, for example, has famously rigorous data protection laws; Spain's data protection act mandates the complexity of passwords. Member States have then applied their own regulatory approach, so that countries such as the UK and Ireland are perceived as traditionally having a relaxed, hands-off approach to enforcement, whereas France and Germany are quick to apply tough penalties for data protection infringements."

Then we have the added complexity of international data protection laws, and how organizations in EU Member States interact with other countries, in particular the US, which has a 'sectorial' approach to privacy. The Article 29: Data Protection Working Party was set up under the Directive of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (visit http://ec.europa.eu/). Hence, personal data cannot be transferred out of the EU to other countries unless suitable legal safeguards are in place, which can be achieved through a number of ways; a decision of 'adequacy' from the European Commission's (EC) Article 29: Data Protection Working

Party to confirm that (a) the destination country has suitable data protection laws and enforcement; (b) 'model clauses' to which all parties subscribe to bring processing under the remit of EU laws and EU courts; (c) 'binding corporate rules' which provide similar controls but permit them to be tailored to fit the specific relationship; or (d)'explicit consent' from the data subject to the transfer and processing (something which is much harder to achieve and manage than might be first thought).

Information technology industries encouraged the EC and the US Department of Commerce to negotiate a new agreement to replace the 'Safe Harbor' Framework by Jan. 31, 2016, deadline set out by EU Member State data protection authorities following the Chief Justice of EU's ruling. Thus, in the case of US transfers, organizations can now use the "US-EU Privacy Shield," a legal framework to which organizations can subscribed to achieve similar outcomes. Recently, Sotto and Hydak (2016) described the process as: "The EU-U.S. Privacy Shield was announced by the EC and US Department of Commerce as a replacement for the Safe Harbor Framework. The agreement contains three key features: (a) Strong Obligations for Companies' Handling of EU Citizens' Data, (b) Clear Safeguards and Transparency Obligations for U.S. Government Agency Access, and (c) New Redress and Complaint Resolution Mechanisms for EU Citizens." Unfortunately, without an agreement, thousands of companies of all types and sizes (in both Europe and the United States) will face widespread uncertainty and serious impacts to their operations and their ability to conduct business across the Atlantic. We welcome the 'EU-US Privacy Shield' agreement and believe it will provide a basis for companies to reliably move data across the Atlantic, while upholding citizens' fundamental rights to privacy and data protection. Moreover, Ashford (2016) recently stated, **"**In the two weeks since the EU-US Privacy Shield data transfer certification process officially opened, applications by US companies has been slow. Only 40 US firms has been certified under the Privacy Shield transatlantic data transfer program, but this is expected to gain momentum. Uncertainty about how the framework may change, as well as concerns that Privacy Shield may challenge, has resulted in relatively few companies rushing to apply for certification. Another reason there has been no rush to apply for certification is that many US companies waited for Privacy Shield to be adopted and approved before starting work on changing their data handling processes to comply with the new framework."

In Nordic countries, which are not all in the EU, similar privacy laws exist, which acknowledge the use of a personal identity code for each person in an 'ID Card' scheme. As Bhasin (2008) stated, "In Europe, individual countries develop and enact their own laws, based on the Directive, which hold to the principles, but may differ in detail. For example, German law does not permit any unsolicited direct mail communications, which are permitted in the UK, although consumers can request not to receive these." Similar laws also exist in many other countries and are documented by Privacy International (visit www.privacyinternational.org). Shockingly, the issue is not that simple. The claim to privacy is protected in the US, Canadian, and German constitutions in a variety of different ways and in other countries through various statutes. For example, Shah and Zacharias (2010) reported that "Several other countries, such as, UK, Spain, Switzerland, Sweden, Australia, China (Taiwan), Thailand, Singapore, to name a few, have enacted laws to protect data and privacy rights." Moreover, Sweden passed legislation that restricts how Web sites can use cookies (Bayardo and Srikant, 2003). The Federal Trade Commission (FTC) has already imposed 20-year privacy agreements on Google and Facebook and is actively investigating other alleged privacy incidents. Meanwhile, a number of bills are also circulating in US Congress to create comprehensive privacy rules for the country. "The federal government has the power to pass a privacy law that could bring about a fundamental shift in how companies collect and use personal data. Most Western countries have already created federal privacy commissioners to protect consumers and to spread awareness about privacy issues in general," said Robert (2011). Some leading Internet companies (especially advertisers) are implementing their own measures to address consumer privacy issues. For instance, Digital Advertising Alliance, which represents dozens of major media and tech companies, has created a system where internet users can view which companies are monitoring their web surfing and even instruct them to stop

serving targeting ads. They hope to create a "Better Business Bureau" type system that encourages best practices and excludes bad actors.

Privacy Regulative Scenario in Select Countries: An Overview

"Privacy laws & rules vary widely throughout the globe, and navigating this thicket of laws is very critical to international commerce. Legislatures across the globe have, therefore, taken notice of such wide disparity and tried to minimize the invasion of privacy," said Bhasin (2007). On the surface, it seems obvious that privacy rights should be protected, but the common standard (law & rules) applied significantly differs from country to country. We are surveying below the privacy legislation scenario prevalent in some prominent countries, such as, Australia, the United States (US), the European Union (EU), Canada, Japan, India, Malaysia, Singapore and Hong Kong. As Slyke and Belanger (2012) optimistically stated, "It is expected that a growing number of countries will adopt privacy laws to foster e-commerce."

Australia

There is no statutory definition of privacy in Australia. Privacy in Australian law is the claimed right of natural persons to protection from intrusion into their personal lives and to control the flow of their personal information. Privacy is not an absolute right; it differs in different contexts and is balanced against other competing rights and duties. It is affected by the Australian common law and a range of Commonwealth, State and Territorial laws and administrative arrangements. While Australia has essentially mirrored the US in respect of regulatory bodies and frameworks to work under, it diverges from the US in respect of legislation in response to data breaches and resulting privacy concerns. Australia is celebrating 2016 as "The Year of Privacy!"

Data privacy/protection in Australia is currently made up of a mix of Federal and State/Territory legislation. The Federal Privacy Act 1988 (Privacy Act) and its Australian Privacy Principles (APPs) apply to private sector entities, with an annual turnover of at least A$3 million, and all Commonwealth Government and Australian Capital Territory Government agencies. The Privacy Act was last amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which came in to force on 12 March 2014. The amendments significantly strengthened the powers of the Privacy Commissioner to conduct investigations (including own motion investigations), ensure compliance with the amended Privacy Act and, for the first time, introduced fines for a serious breach or repeated breaches of the APPs. As Srinivas (2015) reported, "Australian States and Territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies (and private businesses' interaction with them). Additionally, there are no industry specific acts or regulations like HIPAA, SOX or GLBA. Because of this, some organizations do not know their obligations in relation to these laws." These acts are:

- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania), and
- Privacy and Data Protection Act 2014 (Victoria).

There is also various other State and Federal legislation that relates to data protection. For example, the Telecommunications Act 1997, the National Health Act 1953, the Health Records and Information Privacy Act 2002 (NSW), the Health Records Act 2001 (Vic) and the Workplace Surveillance Act 2005 (NSW) all impact privacy/data protection for specific types of data or for specific activities. Private sector entities are referred to as 'organizations'. Under the Privacy Act/the APPs, an organization can be an: individual, body corporate, partnership, other unincorporated association, or a trust.

The United States of America (USA)

In the United States, the claim to privacy is protected primarily by the First Amendment, which guarantees freedom of speech and association. Fourth Amendment provides protection against unreasonable search and seizure of one's personal documents or home, and the guarantee of due process of law. The Federal Trade Commission (FTC, 2010) supports industry self-regulation for online privacy. While 'Fair Information Practices (FIP)' do not themselves carry the force of law, they provide a set of principles for legislation and government oversight. In this way they are similar to the Universal Declaration of Human Rights, in which Article 12 states the principle that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks but leaves the specific legal implementations of those ideals in the hands of individual nations." The five FIPs the FTC adopted in 1973—notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress—are a subset of the eight protections ensconced in the Organization for Economic Co-operation and Development (OECD) 'Guidelines on the Protection of Privacy and Trans-border Data Flows of Personal Data' (OECD, 1980). The FIP of notice underlies the notion of privacy policies, which are mechanisms for companies to disclose their practices. The FTC was concerned that the FIP of notice/awareness was not faring well on the new Internet: consumers did not know where their data went or what it might be used for.

The claim that privacy is protected in the U.S. is based on a regime called "Fair Information Practices (FIP)". FIP is a set of principles governing the collection and use of information about individuals; they are based on the notion of "mutuality of interest" between the record-holder and the individual. The individual has an interest in engaging in a transaction, and the record-keeper—usually a business or government agency—requires information about the individual to support the transaction. Once gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, The Federal Trade Commission (FTC) restated and extended the original FIP to provide guidelines for protecting online privacy. **Table-2** describes the FTC's "Fair Information Practice Principles." According to Wirtz et al., (2007), "In spite of these recent developments, many online businesses, especially in emerging markets, still collect information without consumers' knowledge and consent and do not satisfy the FTC's five principles of sound privacy policies."

Table-2: Federal Trade Commission's Fair Information Practice (FIP) Principles

Notice/Awareness (core principle):	Web sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of data.
Choice/Consent (core principle):	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties.
Access/Participation:	Consumers should be able to review and control the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security:	Data collection must take responsible steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement:	There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violation, or federal statutes and regulations.

According to 'Internet Policy Task Force Report' 2010, "There is no comprehensive federal privacy statute that protects personal information. Instead, a patchwork of federal laws and regulations govern the collection and disclosure of personal information and has been addressed by Congress on a sector-by-sector basis." Federal

laws and regulations extend protection to consumer credit reports, electronic communications, federal agency records, education records, bank records, cable subscriber information, video rental records, motor vehicle records, health information, telecommunications subscriber information, children's online information, and customer financial information. For example, Stevens (2011) contend that "this patchwork of laws and regulations is insufficient to meet the demands of today's technology." The FTC's FIP are being used as guidelines to drive changes in privacy legislation. In July 1998, the U.S. Congress passed the Children's Online Privacy Protection Act (COPPA), requiring Web sites to obtain parental permission before collecting information on children under the age of 13. The FTC has recommended additional legislation to protect online consumer privacy in advertising networks, such as, DoubleClick, which collect records of consumer Web activity to develop detailed profiles that are then used by other companies to target online ads (Krill, 2002). Other proposed e-commerce privacy legislation is focusing on protecting the online use of personal identification numbers, such as social security numbers, limiting e-mail, and prohibiting the use of "spyware" programs that trace online user activities without the users' permission or knowledge.

Table-3: Federal Privacy Laws in the United States

Central Federal Privacy Laws	Privacy Laws Affecting Private Institutions
Freedom of Information Act, 1966	Fair Credit Reporting Act of 1970 Family Educational Rights and Privacy Act, 1974
Privacy Act, 1974	Rights to Financial Privacy Act, 1978
Electronic Communications Privacy Act, 1986	Privacy Protection Act, 1980
Computer Matching and Privacy Protection Act, 1988	Electronic Communications Privacy Act, 1986; Cable Communications Policy Act of 1984
Computer Security Act, 1987	Video Privacy Protection Act, 1988
Federal Managers Financial Integrity Act, 1982 Driver's Privacy Protection Act of 1994 E-Government Act of 2002	Children's Online Privacy Act, 1998 Health Insurance Portability and Accountability Act of 1996 Financial Modernization Act (Gramm-Leach-Bliley Act) of 1999.

(Source: Laudon, K.C. and Laudon, J.P. "Management Information Systems: Managing the Digital Firm," Pearson, 2016)

Table-3 describes the major U.S. federal statutes that set forth the conditions for handling information about individuals in such areas as credit reporting, education, financial records, newspaper records, and electronic communications. Privacy protections have also been added to recent laws deregulating financial services and safeguarding the maintenance and transmission of health information about individuals. The Privacy Act of 1974 has been the most important of these laws, regulating the federal government's collection, use, and disclosure of information (see https://epic.org/privacy/1974act). At present, most U.S. federal privacy laws apply only to the federal government and regulate very few area of the private sector. Recently, Cobb (2016) examined the development of data privacy legislation in the US as an ongoing balancing act, with security interests on one side, and the interest of the individual on the other. The complex and arguably incomplete nature of US data privacy law is often criticized by countries that have more comprehensive data protection legislation." In the U.S., while there has been substantial interest in data privacy issues, efforts have been piecemeal. The Privacy Act, 1974 regulates federal government record keeping, and there are statutes, which regulate specific personal data, such as credit reports, bank records, and videotape rental records.

"In general, self-regulation by the information industry, along with technological privacy protection measures, has been favored. However, a number of information industry groups have issued voluntary codes of conduct and guidelines for fair information collection by their members," says Bhasin (2005). According to 'World Privacy Form Report,' 2011, "The privacy self-regulation programs reviewed in this report were effectively a Potemkin village of privacy protection. Erected quickly, the schemes were designed to look good from a distance. Upon closer inspection, however, the protections offered were just a veneer. The privacy Potemkin village fell-down soon after the gaze of potential regulators drifted elsewhere. Efforts such as the Individual

Reference Service Group (IRSG) and the National Advertising Initiative (NAI) are examples of classic, failed privacy self-regulatory efforts. These and other poorly designed privacy self-regulation schemes had limited market penetration and insufficient enforcement. Still, that was enough to fend off regulators until political winds blew in other directions." However, in some cases, mandatory codes of conduct have recently been adopted. For example, mandatory guidelines were issued by the IRSG, which includes companies, such as Leis-Nexis, who sell personal data via their online services; the three credit reporting companies, Equifax, Experian, and Trans Union; and other companies that sell personal information (Culnan, 2002). The IRSG guidelines require that "annual compliance audits be conducted by independent third parties," and the guidelines prohibit members that are information suppliers from selling data to those found violating the guidelines. As Bhasin (2006) reported, "Most recent privacy concerns have centered on the Internet. Privacy laws in the U.S. are significantly more lax, especially with regard to non-government organizations. Further, governments are significantly more limited in the collection and dissemination of private data than are private businesses." Law does not limit businesses that are not financial institutions or medical organizations. The U.S. approach has been to expect businesses to impose self-regulation on data collection through the Internet. Whether or not this has happened to any significant degree is questionable. The U.S. government, however, has stepped in despite limitations, and Congress has adopted some laws to curb violation of privacy. To strengthen the foundation of commercial data privacy in the United States, we recommend "the consideration of the broad adoption of comprehensive Fair Information Practice Principles (FIPPs)." This step may help close gaps in current policy, provide greater transparency, and increase certainty for businesses. The principles that constitute comprehensive statements of FIPPs provide ample flexibility to encourage innovation. Recently, Geller (2016) concluded: "The US uniquely benefitted from a 'safe harbor' provision that allowed domestic companies to self-certify that they comply with certain principles relating to: notice (when personal information is collected); the choice to opt out of such collection, and access to data collected. The safe harbor law further required such data to be kept secure; to be used only for a specified purpose; and to be kept from being recklessly transferred to third parties. Finally, U.S. companies in the safe harbor program had to implement ways for Europeans to enforce their rights under the provision."

According to Bauer et al., (2012), "Google is forced to wipe a Spanish citizen's past financial troubles from its records. The Belgian Privacy Commission tells Facebook it must 'bend or break' to abide by the country's privacy laws. A plaintiff presses privacy cases against Facebook in both Austrian and European courts." In each instance, national privacy laws collide with the international nature of the Internet, and with American business expectations. Cross-border issues of the online world are not new. Then came to light the notorious case of Edward Snowden. His 2013 exposé of spying practices revealed the U.S. was secretly collecting protected European data, often via U.S. companies like Facebook. The global community upped the ante in response, with new laws proposed or enacted in countries as diverse as Madagascar, Thailand, and Chile. In Europe, individual countries have used the 1995 law to challenge American practices, and the European Commission plans changes to the law it claims will "strengthen online privacy rights and boost Europe's digital economy (Geller, 2016).

The United States has about 20 sector specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories. For example, California alone has more than 25 state privacy and data security laws. These laws, which address particular issues or industries, are too diverse to summarize fully in this paper. In addition, the large range of companies' regulated by the Federal Trade Commission (FTC), are subject to enforcement if they engage in materially unfair or deceptive trade practices. The FTC has used this authority to pursue companies that fail to implement reasonable minimal data security measures, fail to live up to promises in privacy policies, or frustrate consumer choices about processing or disclosure of personal data.

The European Union (EU)

The right to data protection and the right to privacy are two distinct human rights recognized in the Charter of Fundamental Rights of the European Union, the Treaty on the Functioning of the EU (TFEU), and in two legal instruments of the Council of Europe, to which all the EU Member States are parties. One of the first attempts to legislate on privacy matter came in the late 1960s from the Council of Europe, which sought to ensure that the European Convention on Human Rights conferred on individuals the right to protect personal information. Several Member states of the E.U. subsequently passed legislation protecting the fundamental rights of individuals, and in particular, their right to privacy from abuse is resulting from data processing (i.e. the collection, use, the storage, etc.)

"Historically, Europeans have been much more concerned about privacy issues than Americans, and most European countries have enacted very specific & strict laws designed to protect their citizens," says Bhasin (2006a). Unlike the US, European countries do not allow businesses to use personally identifiable information without consumers' prior consent. The European Union (E.U.) adopted the "Directive on Data Protection (Directive 95/46/EC)" in Oct. 1998, which limits any collection and dissemination of personal data. In the E.U., a directive is framework of law; each member nation must legislate more restrictive law; but not a more relaxed one. The directive imposes the same rules in all 30 plus member countries of the E.U. These countries have passed laws that reflect Directive 95; some are even more restrictive. The directive provides that no one collect data about individuals ("subjects") without their permission; that the collecting party notify the subject of the purpose of the collection; that the maintainers of the data ask for the subject's permission to transfer the subject's data to another party; and that upon a proper request from the subject, data about the subject be corrected or deleted. The directive prohibits the transfer of personal data from E.U. countries to any country that does not impose rules at least as restrictive as those of the directive.

Companies operating from the EU countries are barred by law from trading with the US companies that do not abide by the European privacy laws. To overcome the problem, the US government offered to create a list of US companies that voluntarily agree to obey these laws. This list is referred to as a **"**Safe Harbor" (European Organization for Security, 2010). A safe harbor is a legal provision that provides protection against prosecution. Now, European businesses have a protection against prosecution if they deal with US businesses that signed up as members of the arrangement. This arrangement is an official agreement between the United States and the European Union. A European company can look up a US business on the list, which is published online, to see if that business participates. US organizations must comply with the seven safe harbor principles, as spelled out by the US Department of Commerce. However, months after the safe harbor was established very few US companies had signed up. The European Union Privacy Directive has important implications both for companies engaged in e-commerce and for multinational corporations with offices in EU countries. It is based on the idea that collecting and using personal information infringes on the fundamental right to privacy. The directive covers a wide variety of data that might be transmitted during the normal course of business. Although the directive officially covers only personal data, it defines that to mean "any information relating to an identified or identifiable natural person". Organizations that want to trade in EU countries must guarantee that personal information is processed fairly and lawfully; that it is collected for specified, legitimate purposes; is accurate and up-to-date; and is kept only for the stated purpose and nothing more. "The indirect effect of this rule is to induce the countries interested in having commercial relations with the EU to adopt similar data protection laws. In the absence of these laws, local companies are not be able to work with European partners, because they cannot receive personal data concerning consumers, suppliers and partners. Faced by the choice between adopting European standards on data protection or losing commercial relations requiring trans-border data flow, the United States has also come to terms with the European Commission" (Mantelero, 2012).

As Goldfarb and Tucker (2011) observed, "Substantial rights are given to individuals regarding the information that organizations possess about them. Individuals must have access to any personal information collected, and

any mistakes must be corrected. More important, individuals may prohibit the use of their personal information for marketing purposes." One recent study suggested that E.U. Privacy Directive impacts numerous parts of an organization's records. A partial list of business includes human resources, call centers, customer service, payment systems, sale of financial services to individuals and business, personal and corporate credit reporting, as well as accounting and auditing. According to EU Commission (2011), "All forms of transmission are covered, including electronic and hard copy. In European Union's initial analysis, the U.S. was not listed among those countries seen as adequately protecting the privacy of personal data. Now, over 350 organizations are on the Department of Commerce's Safe Harbor List." In January 2012, the European Commission proposed a major overhaul of the existing legislative framework on the protection of personal data. The reform was necessitated mainly by three factors: (a) new challenges posed by globalization and Internet developments in the area of online services, which impact the processing of personal data and endanger the privacy of individuals; (b) a new legal basis in the TFEU; and (c) a dramatic increase in Internet users and serious concerns expressed by 70% of individuals in the EU about the possible misuse of their personal data.

According to Morando et al., (2014), "It could be argued that the European Commission (EC) proposal for a General Data Protection Regulation is far more 'Internet-aware' than its predecessor (still in force, Directive 95/46/EC), by taking into account challenges related to data exchange happening online. Several rules are being enhanced, e.g., ex ante privacy assessment for the data controller, new requirements in terms of 'privacy by design' and 'privacy by default' measures, as well as stronger sanctions in case of breach. Moreover, new rights are being introduced, such as data portability (Article 18), for which the data subject has the right to obtain from the data controller a copy of the data, and transfer it to another information system. While the measures may be effective in some regards, there is reason to question if the underlying assumptions about user's valuation of privacy are being taken into account sufficiently." Recently, Weiss and Archick (2016), remarked, "In October 2015, the Court of Justice of the European Union (CJEU, which is also known as the European Court of Justice, or ECJ) invalidated the Safe Harbor Agreement. The CJEU essentially found that Safe Harbor failed to meet EU data protection standards, in large part because of the U.S. surveillance programs. Given that some 4,500 U.S. companies were using Safe Harbor to legitimize transatlantic data transfers, U.S. officials and business leaders were deeply dismayed by the CJEU's ruling. Companies that had been using Safe Harbor as the legal basis for US-EU data transfers were required to immediately implement alternative measures. Experts claimed that the CJEU decision created legal uncertainty for many U.S. companies and feared that it could negatively impact U.S.-EU trade and investment ties. On Feb. 2, 2016, U.S. and EU officials announced an agreement, "in principle," on a revised Safe Harbor accord, to be known as 'Privacy Shield'; the full text of the agreement was released on Feb. 29, 2016. The US and EU officials assert that the new accord will address the CJEU's concerns. In particular, they stress that it contains significantly stronger privacy protections as well as safeguards related to US government access to personal data."

Canada

In Canada, there are 28 federal, provincial and territorial privacy statutes (excluding statutory torts, privacy requirements under other legislation, federal anti-spam legislation, identity theft/ criminal code etc.) that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, and remedies and enforcement provisions, they all set out a comprehensive regime for the collection, use and disclosure of personal information. The summary below focuses on Canada's private sector privacy statutes:

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Personal Information Protection Act (PIPA Alberta)
- Personal Information Protection Act (PIPA BC),
- Personal Information Protection and Indentity Theft Prevention Act (PIPITPA) (not yet in force), and

- An Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act), (collectively, 'Canadian Privacy Statutes').

The 'PIPEDA' applies: (a) to consumer and employee personal information practices of organizations that are deemed to be a 'federal work, undertaking or business' (e.g., banks, telecommunications companies, airlines, railways, and other interprovincial undertakings); (b) to organizations who collect, use and disclose personal information in the course of a commercial activity which takes place within a province, unless the province has enacted 'substantially similar' legislation (PIPA BC, PIPA Alberta and the Quebec Privacy Act have been deemed 'substantially similar'), and (c) to inter provincial and international collection, use and disclosure of personal information. PIPA BC, PIPA Alberta and the Quebec Privacy Act apply to both consumer and employee personal information practices of organizations within BC, Alberta and Quebec, respectively that are not otherwise governed by PIPEDA.

Like members of the European Union, Canada established a privacy commissioner. The privacy commissioner is an officer of Parliament, reporting directly to Parliament. Under the act, individuals may complain to the privacy commissioner about how organizations handle their personal information. The commissioner functions as an ombudsman; initiates, receives, investigates, and resolves complaints; conducts audits; and educates the public about privacy issues. He or She has two sets of powers—the power of disclosure, which is the right to make information public; and the power to take matters to the Federal Court of Canada, which can in turn order organizations to stop a particular practice and award substantial damages for contravention of the law. Recently, the Office of the Privacy Commissioner of Canada (2016) stated, "Technology is now moving far too quickly for privacy regulators to keep pace. There are several technologies involved in the Internet of Things, such as radio-frequency identification (RFID), near-field communications (NFC), machine-to-machine communication (M2M) as well as wireless sensor and actuator networks."

Japan

Japan is a member of APEC and as such subscribes to its approach to privacy. Japan also has a privacy act, which regulates government data collection practices, but with regard to private sector information handling, the government has preferred voluntary guidelines issued by the government ministries rather than legislation. These include the Ministry of Finance, which issued guidelines in March 1986 on Information Handling relating to the Establishment or Use of Credit Information Agencies by Financial Institutions; the Ministry of International Trade and Industry, which issued guidelines in March 1986 on Consumer Credit Information Management; the Ministry of Posts and Telecommunications, which issued Guidelines on Personal Data Protection in Telecommunications in Sept. 1991, and which issued Guidelines on the Protection of Subscriber Personal Data for the Audience of Broadcast Services in Sept. 1996.

Japan also recently passed its first omnibus privacy law, which is "a middle-way between the industry-sector-based privacy laws of the U.S. and the comprehensive data protection laws of the European Union." The P&AB offers the Guide to Consumer Privacy in Japan and the New Japanese Personal Information Protection Law to explain the data-protection climate in Japan and help companies navigate the legislation (Laudon and Traver, 2014). The president signed the "Protection of Personal Information Act" (Popi) and it became law on Nov. 26 2013. Popi essentially regulates how anyone who processes personal information must handle, keep and secure that information. It may have taken over eight years to complete, but the final result is a good piece of legislation. Popi is strict and has substantial penalties. Anyone who contravenes Popi's provisions faces possible prison terms and fines of up to R10-million. Popi also allows individuals to institute civil claims so there's the possibility of further financial loss on top of any fine that may be imposed (Pierce, 2013). The Act requires business operators who utilize for their business in Japan a personal information database which consists of more than 5,000 individuals in total identified by personal information on any day in the past six months to

protect personal information. Amendments to the APPI, which were passed in 2015 and go into effect no later than Sept., 2017 (the 'Amendments'), apply the APPI to all businesses in Japan, regardless of whether the business operator maintains a database of more than 5,000 individuals.

Further, the Amendments clarify the definition of personal information, add two new classes of information, and introduce new requirements for 'opt-out' choice for business operators to disclosure personal information to third parties. Finally, as of Jan. 1, 2016, the Amendments created a Privacy Protection Commission (the 'Commission'), a central agency which will act as a supervisory governmental organization on issues of privacy protection. The Amendments must be enacted no later than Sept. 2017, so the Amendments could go into effect at an earlier date.

India

India is party to a number of international instruments containing privacy protections. These include: The Universal Declaration on Human Rights (Article 12), and The International Convention on Civil and Political Rights (Article 17). The Constitution of India does not specifically guarantee a "right to privacy (Ahmad, 2009). However, through various judgments over the years the Courts of the country have interpreted the other rights in the Constitution to be giving rise to a (limited) right to privacy–primarily through Article 21–the right to life and liberty. The constitutional right to privacy in India is not a very strong right in itself and is subject to a number of restrictions. According to Bhasin (2006b), "The fundamental rights, as engrained in the Constitution of India, come closest to protecting an individual's privacy and his freedom of expression. Just as the freedom of speech and expression is vital for the dissemination of information on matters of public interest, it is equally important to safeguard the private life of an individual to the extent that it is unrelated to public duties or matters of public interest. The law of privacy, therefore, endeavors to balance these two competing freedoms." The right to privacy has been interpreted as an unarticulated fundamental right under the Constitution of India. The growing violation of this right by the State on grounds (that are not always bona fide) encouraged the Indian Judiciary to take a pro-active role in protecting this right.

There is no 'specific' legislation on privacy and data protection in India. However, the "Information Technology Act," 2000 (the 'Act') contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically). India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules). Here, Bhasin (2015**)** stated, "The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal data, including sensitive personal information to comply with certain procedures. It distinguishes both 'personal' information and 'sensitive' personal information." In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organization providing services relating to collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is not subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services. Thus, in 2011, India passed a new privacy package that included various new rules that apply to companies and consumers. A key aspect of the new rules requires that any organization that processes personal information must obtain written consent from the data subjects before undertaking certain activities. Application of the rule is still uncertain. Previously, the Information Technology (Amendment) Act, 2008 made changes to the Information Technology Act, 2000 and added the following two sections relating to Privacy: (a) Section 43A, which deals with implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain. (b)Section 72A, which provides for

imprisonment for a period up to 3 years and/or a fine up to Rs. 5,00,000 for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract.

There is a preconceived assumption that privacy laws in India are 'notoriously' weak. Protection afforded to personal data in India may not be considered adequate, as compared to the global standards set by various governments and institutions across the globe. However, there are distinct differences in the concept of privacy that we understand in India vis-à-vis the approach of the Western countries. "This unquestioned assumption is based on a paradigm that does not take into consideration that the conception of privacy in India is influenced by its culture of trust" (Basu, 2010). Generally, Indian society and culture is one of openness, and the concept of protecting one's identity from society is rather alien. However, this is not the position in Western nations, where personally identifiable data has been widely used to target minorities, fight wars, used for telemarketing purposes, committing financial frauds and scandals, and so on. However, some market players in India have already started misusing the general openness of Indian society to market credit-cards, sell personal information, send Spam e-mails, conduct illegal background checks on persons, etc. In this context, it would be necessary to balance the unique nature and needs of Indian society with the privacy and protection principles as expounded by the Indian Constitution. According to Yadav (2015), "Amid the raging controversy over alleged snooping, the Centre said it is giving the final touches to the Right to Privacy Bill, 2014, which aims at protecting individuals against misuse of data by government or private agencies. The draft Bill has clearly stated that the right to privacy is part of the right of a person under Article 21 of the Constitution and no person can disclose the sensitive personal data without the prior consent of the data subject (person whose data is collected)."

The fate of India's data privacy legislation and its ID system are intertwined, both depending on whether India's Supreme Court decides that India has an implied Constitutional right of privacy, and whether it extends to data privacy. In a decision in the Puttaswamy Case, in August 2015, a three judge bench of India's Supreme Court (i) referred to a 'constitution bench' of at least five Justices the existence and content of the constitutional right of privacy; and (ii) in the interim, allowed India's 'Aadhaar' ID number system to continue operating, despite its alleged interference with privacy, but with limitations on how it may be employed (Greenleaf, 2015a). Unfortunately, there are no specific national regulators dealing with administration of privacy laws in India. However, the Privacy Bill contemplates the creation of a Data Protection Authority of India which will monitor and enforce compliance with the Bill. In cases where the compensation amount claimed for a failure to protect confidentiality of sensitive personal information is less than Rs. 50,000,000, the IT Act provides for the Government to appoint an Adjudicating Officer. All proceedings before the Adjudicating Officer are deemed to be judicial proceedings and the officer has the powers of a civil court. The details of the enquiry procedure that the Adjudicating Officer must use are provided in the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules (2003). This time around, the telecom regulator is looking to kick-start debate over the challenges that arise in regulating the flow of data through the numerous cloud-based platforms that underpin our digital life. Questions of cross-border flow of data, licensing of cloud-based services and best practices on how to successfully carry out law-enforcement requests are a few examples. "Regulations should be put in place to protect the interests of both cloud services providers and the consumers. Regulations are also required for standardization of technical parameters associated with cloud computing networks (Srivas, 2016).

India does have a separate dedicated law to protect right to privacy nonetheless the Information
Technology Act, 2000 provides a comprehensive protection of data and prescribes stern punishment for its breach. The stand of academicians and scholars for stronger data protection law is fulfilled by the Information Technology Act, 2000 along with its rules. Even though Information Technology Ac, 2000 has extraterritorial jurisdiction, however, its rules are applicable to corporate body located in India. Hence the concept of data

protection under Information Technology Act, 2000 lags behind on jurisdictional issues. Further the requirement of business process outsourcing companies which handle large amount of personal sensitive information is different from other industries is not specifically addressed by the Act. The growing health care sector also requires specific legislation to protect medical privacy of patients, which is also not explicitly addressed by the Information Technology Act, 2000. Thus,
It can be concluded that the dedicated data protection law is the need of the hour and requirement
of industry and citizen (Kolekar, 2015).

In the privacy and data protection area, the winds of change are blowing across India, and they are likely soon to alter the landscape. But the new shape of that landscape is not yet clear. The near future is likely to see major modifications to the Information Technology Act 2000 and/or a proposal to the EU for a Safe Harbor–India regime. The long-term shape of Indian data protection law may depend on the success (or lack of it) that the short-term solution enjoys. But, one way or another, Indian privacy law is likely to change dramatically in the next few years.

Malaysia

Malaysia's first comprehensive personal data protection legislation, the "Personal Data Protection Act, 2010" (PDPA), was passed by the Malaysian Parliament on 2 June, 2010 and came into force on 15 Nov., 2013. The law applies to the processing of "personal data" by entities operating in Malaysia but generally does not apply to data processed entirely outside of Malaysia. Additionally, official registration requirements will extend to many classes of "data users" (those who control or authorize data processing), including those in the communications, banking and financial, insurance, health care, and other industries. "Personal data" is defined broadly within the Act as "any information in respect of commercial transactions" relating to any person "who is identified or identifiable from that information," either by itself or in combination with other data.

The law is structured around seven principles viz., 'general' (to protect legal rights or comply with legal obligations, or to protect the "vital interests" of the data subject), 'notice and choice' (extensive and detailed disclosures to affected data subjects about the use of their data, the source of the data, the kind of data being processed, the data subject's rights to access or inquire about his data, and more), 'disclosure' (disclosure must be limited by the purpose for which the data was originally collected, or, if data is disclosed to third parties, it may only be disclosed to third parties whose identity has itself been disclosed to the data subject in an appropriate notice), 'security'(data users to take "practical steps" to protect personal data from loss, misuses, modification, unauthorized or accidental access or disclosure, alteration or destruction), 'retention' (data may only be retained for so long as is necessary to fulfill the purpose for which it was collected), 'data integrity' (data user must take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-to date) and 'access' (data subjects have the right to access and correct their personal data). "Further, the law imposes cross-border transfer restrictions and on the handling of personal data that is used in direct marketing. The Act imposes criminal penalties for violations, which may include fines as well as imprisonment," (Chew, 2015).

In August 2015, we reported on the Malaysian 'Personal Data Protection Commission' (PCPD) publishing its consultation paper on data protection and three new draft standards on data security, data retention and data integrity (the Draft Standards). It was the first time the PDPC had opted to use it power to produce legally binding standards under the Personal Data Protection Act 2010 (the PDPA). On 23 Dec. 2015, the Personal Data Protection Commissioner ("Commissioner") published the Personal Data Protection Standard 2015 after consulting members of the public. The Standard sets out the minimum standards to process personal data and it is applicable to anyone who processes or has control or authorizes the processing of any personal data relating to commercial transactions. Broadly, it sets out the security standards (electronic and non-electronic

processing), retention standards and integrity standards. Following this, on 23 Dec. the Personal Data Protection Standards 2015 (the Standards) came in to force. Data protection principles are a new concept to Malaysia and the Standards' prescriptive format aims to clarify certain elements of the PDPA in order to provide organizations with guidance for implementation. As Majid (2016) stated, "Generally, the Standards are similar to the Proposed Standards, with minor changes. As the Standards are already in force, companies are urged to comply, since any contravention could lead to a fine not exceeding RM250, 000 or imprisonment for a term not exceeding two years, or both."

Singapore

While Europe, for example, has human rights as the underpinnings of its data protection laws, Singapore is not shy about admitting its laws are about securing the country's place in the global economic marketplace. Singapore has modern digital economy laws in most areas. For example, the Electronic Transactions Act 2010 implements the United Nations Convention on Electronic
Contracting, which Singapore has ratified. Singapore also has up-to-date cybercrime laws and intellectual property laws. Singapore privacy law has now come into force, and provides a balanced approach between protecting personal information and facilitating innovation in cloud
computing and the digital economy.

Singapore implemented its comprehensive "European-style" Personal Data Protection Act ("PDPA") in two stages in Jan. and July 2014. Singapore Personal Data Protection Act 2012 (PDPA) is a law that governs the collection, use and disclosure of personal data by all private organizations. The Act has come into full effect on 2nd July 2014. Organizations which fail to comply with PDPA may be fined up to $1 million and suffer reputation damage. Singapore enacted a new "Personal Data Protection Act, 2012 (PDPC)" (No. 26 of 2012) ('Act') on 15 Oct. 2012. The Act took effect in 3 phases:

- Provisions relating to the formation of the Personal Data Protection Commission (the 'Commission') took effect on 2 Jan. 2013.
- Provisions relating to the National Do-Not-Call Registry ('DNC Registry') took effect on 2 Jan. 2014.
- The main data protection provisions took effect on 2 July 2014.

Singapore's new Personal Data Protection Commission has also been very active in taking public consultations about specific requirements under the law and publishing extensive explanatory guidance for businesses and consumers alike. On Sept. 24, 2013, the Singapore Personal Data Protection Commission (the "Commission") published guidelines to facilitate implementation of the Singapore Personal Data Protection Act (the "PDPA"). The Advisory Guidelines on Key Concepts in the Personal Data Protection Act and the Advisory Guidelines on the Personal Data Protection Act for Selected Topics provide explanations of concepts underlying the data protection principles in the PDPA, and offer guidance on how the Commission may interpret and apply the PDPA with respect to certain issues. The guidelines are advisory only; they are not legally binding. The PDPC is particularly focused on helping SMEs comply with the law. According to Pfeifle (2015), "Commissioner Leong stated the PDPC is tasked with helping companies "exploit the benefits of big data while still complying with the PDPA (Personal Data Protection Act)," for example. He also noted that when data breaches happen, "it is not only personal data that is lost. Reputations of individuals and organizations are involved as well." As Parsons and Colegate (2015) pointed out, "Singapore's new law has been enacted with some of the stiffest penalties for data privacy offences in the region, with fines of up to S$1 million (USD800, 000). It is also clear that the new Commission will be resourced to enforce the law, a view reinforced in November by the announcement that it would be appointing a panel of digital forensic experts to help investigate data security breaches."

Despite having been established only recently, the Commission has been considerably active in issuing proposals for advisory and regulatory materials in preparation for next year's implementation dates. In early Feb. 2013, the Commission proposed advisory guidelines on selected topics and key concepts, and issued proposals for regulatory matters and for the operation of the Do Not Call registry. The Commission also has hosted events to help organizations develop an understanding of the PDPA ahead of upcoming implementation dates. The PDPA's provisions establishing protections for personal data are scheduled to become effective on July 2, 2014. Certain other provisions establishing a Do Not Call registry will become effective earlier next year.

Singapore's PDPA is structured to serve as a framework law: the law sets forth the minimum, fundamental rules necessary to establish a data protection framework. More detailed regulation on particular topics (such as whether particular information should be defined as "sensitive personal information" and whether more stringent rules should apply to such information) is subject to sectorial rulemaking. Accordingly, we can expect Singapore authorities to issue additional, more specific, regulations on a rolling basis. Singapore's Personal Data Protection Commission (PDPC) is stepping up its efforts to enforce the Act 2012. The PDPC has also recently announced the need for organizations to improve their data security and data protection measures and has issued new guides primarily focusing on data protection measures, which organizations should consider carefully (Thiel and Biggs, 2016).

Hong Kong

According to Greenleaf (2015), "For 17-years, Hong-Kong's 1995 Personal Data (Privacy) Ordinance, the first comprehensive data privacy law in Asia, remained without substantial amendments. The Amendment Bill of 2012, in force since April 2013, involved fewer changes than were recommended by Hong Kong's Privacy Commissioner. Two-and-half-years later the stronger enforcement regime is still only being applied cautiously. However, the Commissioner and the tribunal administering the Ordinance have both given its substantive principles increasingly strong interpretations." Hong Kong's Privacy Commissioner for Personal Data (PCPD) was the first data protection authority created in Asia. Since Oct. 2011, the Hong Kong Office of the Privacy Commissioner for Personal Data has published three "Guidance Notes" to help data users comply with the Personal Data (Privacy) Ordinance (the "Ordinance"). These Notes are not legally binding, nor are they intended to serve as an exhaustive guide to the application of the Ordinance, but they provide good, practical examples and tips that the Commissioner has developed as it has implemented the Ordinance. On June 27, 2012, the Hong Kong Legislative Council passed a bill to amend the Personal Data (Privacy) Ordinance (the "Ordinance"). The amendment will become effective in phases. Most provisions will become effective on October 21, 2012. The Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong) (Ordinance) regulates the collection, use and handling of personal data by data users.

In Hong Kong, the Personal Data (Privacy) Ordinance (Cap. 486) regulates the collection and handling of personal data. Enforcement is through the Office of the Privacy Commissioner for Personal Data (PCPD). The Ordinance was significantly amended by the Personal Data (Privacy) (Amendment) Bill in July 2012. Most of the amendments introduced by the Bill came into force on October 1, 2012. Two major areas of amendments, namely new restrictions against the use and provision of personal data in direct marketing, and new powers of the PCPD to provide legal assistance to persons in civil proceedings have also come into force on April 1, 2013. Hong Kong's Privacy Commissioner for Personal Data is very much an activist regulator. He publicly comments on developments in privacy law abroad and continues to press for wider ranging regulation enforcement powers under the PDPO. This activist approach continued throughout 2014. "The trend towards Bring Your Own Device ("BYOD") has come to the attention of Hong Kong's Privacy Commissioner. The Commissioner published an information leaflet on 31 August 2016, which highlights the risks of data breaches where employees are using their own mobile phones or other personal devices to access work emails/systems,

and suggests best practices for organizations allowing BYOD. The Commissioner has suggested as best practice that organizations should conduct risk assessments and implement internal BYOD policies accordingly to ensure appropriate data privacy and data security compliance" (Thiel and Biggs, 2016a).

Twenty-year is a long-time for any law to remain on the statute books without being implemented. That is how long Section 33 of Hong Kong's Personal (Data) Privacy Ordinance (PDPO) has been waiting for implementation. Sec. 33 prohibits the cross-border transfer of personal data from Hong Kong unless certain exceptions apply or the data is transferred to countries where similar data protection laws are in place. Recently, Chan and Allison (2015) have pointed out that "the increased activity from the Privacy Commissioner in relation to Sec. 33 suggests strongly that it may be implemented in the very near future. Whilst the Guidance Note does not have the force of law, it does give a very good indication on how the Privacy Commissioner intends to enforce Sec. 33 when it does come into force. Implementation of Sec. 33 in the near future would be a significant development in Hong Kong's data privacy regime and we expect to see increased activity and communication on this front in the near future."

World Leaders in Privacy: A world in flux

Really speaking, we live in one world, use one internet, but are governed by multiple laws. Some of the very same emerging economies constantly being talked about as "tomorrow's markets" are legislating around data privacy in drastically different ways. Rules and regulations vary widely geographically. There are no consistent guidelines and rules... even neighboring legislative regions have different policies.

The EU's negotiation with the US, in recent years, has seen the continent of Europe painted as the bulwark of data privacy laws. It just happens that because of the developed markets in the EU, which has the most progressive laws on data protection globally, and the US, which has the vast majority of the technology industry benefiting from the creation of data, that the data flow between them is particularly under scrutiny. Europe definitely sets the tone, but it is important to remember that the bloc has defined its reaction to data privacy in relation to the US. That is not an exclusive standpoint. For example, Canada's Digital Privacy Act came into force in 2015 to help guard Canadians' private data stored by US-based services like Facebook, Gmail, Twitter and YouTube, though individual provinces in Canada do have their own requirements (Fuchs, 2011). Canada and Europe tend to lead the world in terms of legislating personal data, but the rest of the world is catching up fast, though hugely unevenly. Many countries outside of the EU have enacted data protection laws in recent years, including Malaysia, South Korea, Singapore, and Turkey. Many of these laws are very similar to the EU Data Protection Directive, although these jurisdictions often carry incredibly heavy sanctions for non-compliance—including prison sentences. However, the European Commission thinks only Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay offer EU citizen's adequate protection.

Some areas of the world have modeled their response to data privacy on the EU's battle with the US, and that certainly applies to Asia, which goes straight to the top of the list of concern for the IT and tech industry (Council of Europe, 2014). In recent years, several Asian countries have undergone a major change in data privacy regulation, and that is mostly due to the Asia-Pacific Economic Co-Operation (APEC) Privacy Framework. APEC agreed on a privacy framework in 2005. Early leaders in Asia Pacific data protection were Australia, New Zealand, and Hong Kong, all of which passed strong data privacy laws in the 1990s. More recently, China, Taiwan, South Korea, Malaysia, Singapore, and the Philippines have passed comprehensive legislation of their own. The APEC Privacy Framework has provided some rough signposts for a common approach to principle-based regulation, but priorities for policymaking and enforcement vary significantly by jurisdiction. However, there are efforts to harmonize Asia and the EU.

Asian privacy laws are country-specific rather than regional. Singapore has much stricter privacy laws, which likely developed because of its historically vibrant banking sector ... but Asia lacks centralized control or standards between data protection authorities. For example, take India whose Information Technology Act was passed 15 years ago. India has passed a principles-based law to protect data privacy. It is a start, but so far it is about specific sectors, not wide-ranging principles. There is a similar scenario in China, which is headed for a data localization model. China has had a national law on the collection of electronic information since 2012. The model China is chasing is perhaps that of Russia. All Russian citizen personal data can only be stored in Russia. A reaction to NSA snooping, the law effectively makes Western technology companies' data on Russian citizens open to snooping by Russian authorities. Elsewhere in Asia there is a lack of blanket rulings, largely in the 'tiger' economies. Some countries, such as Indonesia, have offered very particular rules surrounding the country's attitude to data privacy for years now— the old Blackberry requirements are an example. Another fast growing market, Latin America, is also in flux, with some specific targeted laws, but no blanket protection. Uruguay, Colombia, Costa Rica and Mexico are all still developing their technological base and face speedy evolution in emerging requirements, meaning legislation and policy is difficult to keep up to date.

"When it comes to data privacy law, the world is in flux, and it is unlikely to come to equilibrium any time soon. As much as an approach based on "one size fits all" will not be the solution, many countries will continue to observe what the EU does and seek to select parts of the legislation that work well, leaving the not-so-practical elements," says Bhasin (2016). There are 195 countries worldwide, and each may have their own laws and regulations— it is a complex task to be up to date with every country's laws. Privacy standards may be feeding off each other, and to some extent they are harmonizing, but before you do business in a new country check whether you are collecting data legally. In global data collection, less is always more.

Conclusion

No doubt, privacy laws vary throughout the globe. In the US, Canada, and Germany, rights to privacy are explicitly granted in, or can be derived from, founding documents such as constitutions, as well as in specific statutes. However, Kugler (2015) remarked, "Concerns over online privacy have brought different responses in different parts of the world. In the US, for example, many Web browsers let users enable a Do Not Track option that tells advertisers not to set the cookies through which those advertisers track their Web use. Compliance is voluntary, though, and many parties have declined to support it. On the other hand, European websites, since 2012, have been required by law to obtain visitors 'informed consent' before setting a cookie, which usually means there is a notice on the page saying something like 'by continuing to use this site, you consent to the placing of a cookie on your computer.' Why are these approaches so different?" Common EU rules have been established to ensure that personal data enjoy a high standard of protection everywhere in the EU. As Bhasin (2012) pointed out, "The two main pillars of the data protection legal framework in the EU are: the Data Protection Directive and the ePrivacy Directive (Directive on Privacy and Electronic communications). In fact, the EU has adopted very strict laws to protect its citizens' privacy, in sharp contrast, to 'lax-attitude' and 'self-regulated' law of the US. To avoid disruption of business with the EU and possible litigation, the US businesses can sign on the "Safe harbor" arrangement." An attempt was made to summarize the privacy legislation scenario prevalent in the select countries, such as, Australia, Canada, the EU, the USA, Japan, India, Malaysia, Singapore and Hong Kong. It is hoped that a growing number of countries will adopt privacy laws to foster e-commerce. In nutshell, the privacy scenario in the United States and the European Union remains at best a gradual work-in-progress, and how soon it will attain perfection only future will tell us.

Legislative action, though essential to any comprehensive privacy strategy, is not necessarily guided by the current capabilities and limitations of information technology infrastructures. Privacy legislation that impacts the IT infrastructure is not unique to the US. Sweden recently passed legislation that restricts how Web sites can use cookies, a technology that enables tracking of users across multiple visits. But cookies are also widely used

in e-commerce applications, such as implementing online store shopping carts. As pointed out by Greenleaf (2015b), "By January 2015, the total number of countries with data privacy laws has increased by over 10% to 109. Information access laws have a somewhat similar trajectory to data privacy laws, having reached the 'significant landmark' of laws in 100 countries in mid-2014. The geographical distribution of the 109 laws by region is: EU (28); Other European (25); Africa (17); Asia (12); Latin America (10); Caribbean (7); Middle East (4); North America (2); Australasia (2); Central Asia (2); Pacific Islands (0). So there are now 53 laws in European countries, but (for the first time) a majority of 56 data privacy laws are outside Europe, over 51% of the total. Because there is little room for increase within Europe, the majority of the world's data privacy laws will now continue to be from outside Europe, and increasingly so. During this 18 month period, the fastest 'growth area' has been Africa, with five new laws, including a new Act in Madagascar in January 2015. Data privacy laws are clearly no longer 'a European thing,' though the influence of 'European standards' remains paramount."

As Stevens (2016) pointed out, **"**Our problem is the contextual, changing and culturally sensitive nature of privacy. What works in one organization does not necessarily work in the next; controls that might be appropriate in one country could hinder normal business operations in another; personal data processing that is considered intrusive on one continent might be of no consequence to individuals in another. The new General Data Protection Regulation (GDPR) does include some control objectives, such as the requirement for a data protection officer or use of data protection impact assessments, and it remains to be seen how successfully organizations can respond to these demands. That's why the British Standards Institute's freshly rewritten BS10012 Data Protection Specification for a personal information management system is a welcome development."

The E&Y (2014) 'Privacy Trends' Report asserted that "we are managing privacy in a time where carefully considered, detailed regulatory requirements do not necessarily result in effective privacy or data protection. Today's privacy regulations, as well as those being considered by regulatory bodies around the world, seem completely inadequate to protect individuals from the privacy risks emerging technologies present. Technology innovations, at work and at home, are pushing the limits of privacy well beyond current regulatory standards and legal requirements." No doubt, there is no single solution to the erosion of privacy in cyberspace; no single law that can be proposed or no single technology that can be invented to stop the profilers and surveliants in their tracks. Indeed, the battle of privacy must be fought on many fronts—legal, political, and technological—and each new assault must be vigilantly resisted as it occurs. Privacy in the age of technology is quickly becoming a paradox. Today's privacy regulations, as well as those being considered by regulatory bodies around the world, seem completely inadequate to protect individuals and organizations from the privacy risks technologies present. Here, Bhasin (2016a) says, "while the regulation of privacy will continue to evolve, particularly as technology advances, businesses, agencies and individuals must also step up to the challenge of taking control of privacy management. No doubt, governments across the globe are making valiant efforts to protect privacy, but they cannot do it alone."

Some regulatory mechanisms remain effective, such as the European Union's Binding Corporate Rules (BCR). More often, regulations are outdated almost immediately upon release. And then there are some, such as Safe Harbor—the US–EU framework that has been in place for more than a decade—that are under siege. Recently, Sotto and Hydak (2016) stated, "On Feb. 2, 2016, US and EU officials announced an agreement, "in principle," on a revised Safe Harbor accord, to be known as Privacy Shield." So where does that leave us? How can organizations safeguard privacy in an age of technology? According to Swire et al., (2016), "The answer lies more in governance than regulation, in innovation more than compliance. Organizations need to focus on privacy accountability that follows an ethical path as well as aligning with suggestions from regulators, that adheres to the spirit rather than the letter of any regulation, and that engenders the trust of those whose privacy an organization has pledged to protect rather than erode it by not instilling enough importance in privacy within

the organization." To sum up, technology alone cannot address all the concerns surrounding a complex issue like privacy. The total solution must combine laws, societal norms, markets, and technology. However, by advancing what is technically feasible, we can influence the ingredient mix and improve the overall quality of the solution.

References

Ashford, W. (2016), Slow response to Privacy Shield EU-US data transfer program, *ComputerWeekly.Com*. 15 August.

Ahmad, T. (2009). Right of Privacy: Constitutional Issues and Judicial Responses in USA and India, particularly in Cyber age, available at www.ssrn.com/abstract=1440665.

Bauer, C., Korunovska, J., & Spiekermann, S., (2012). On the value of information - what Facebook users are willing to pay? ECIS 2012 Proceedings. Paper 197. Available at: http://aisel.aisnet.org/ecis2012/197

Basu, S. (2010), Policy-Making, Technology and Privacy in India, *The Indian Journal of Law and Technology*, 6(1), 65-88.

Bayardo and Srikant (2003), Technological Solutions for Protecting Privacy, *Web Technologies*, Sept. 115-118.

Bhasin, M.L. (2005). Challenges of Guarding Privacy—Practices Prevalent in Major Countries, *The Chartered Accountant*, January, 735-745.

Bhasin, M.L. (2006). Guarding Privacy on the Internet, *Global Business Review*, 7(1), January-June, 137-156.

Bhasin, M. L. (2006a). Data Mining: A Competitive Tool for Banking and Retail Industries, *The Chartered Accountant*, October, 588-594.

Bhasin, M.L. (2006b). Privacy Protection on the Internet: Privacy Policy, Government Regulation and Technology Solutions, *Amity Business Review*, July-December, 44-59.

Bhasin, M. L. (2007). Mitigating Cyber Threats to Banking Industry, *The Chartered Accountant*, April, 50(10), 1618-1624.

Bhasin, M.L. (2008). Guarding Privacy on the Internet: Privacy Policy, Government Regulations and Technology Solutions, *International Journal of Internet Marketing and Advertising*, 4(2/3), Special Issue on SME's, 213-240.

Bhasin, M. L. (2012). Online Privacy Protection: Privacy Seals and Government Regulations in Select Countries, *International Journal of Finance and Accounting*, 1(6), Nov., 148-161.

Bhasin, M. L. (2012a). Guarding Online Privacy: Privacy Seals and Government Regulations, *European Journal of Business and Social Sciences*, 1(9), Dec. 2012, 1-20.

Bhasin, M.L. (2015). Menace of Frauds in Banking Industry: Experience of a Developing Country, *Australian Journal of Business and Management Research*, 4(12), April 21-33.

Bhasin, M.L. (2016). Integration of Technology to Combat Bank Frauds: Experience of a Developing Country, *Wulfenia Journal*, Feb., 23(2), 201-233.

Bhasin, M.L. (2016a). Online Privacy Protection: Privacy Seals, Government Regulations and Technological Solutions, *International Journal of Management Sciences and Business Research*, 5(7), July, 86-116.

Bowman, L.M. (2010). House Pulls Carnivore into the Light. *ZDNet News* (23 July).

Chaffey, D. and White, G. (2011). Business Information Management. Prentice-Hall, Financial Times, 2nd edition.

Chew, K.Y. (2015), Data Protection Compliance in Malaysia Set to Cause Headaches to Businesses, *Baker & McKenzie*. Available at http://www.bakerinform.com.

Chan, M. and Allison, D. (2015), Hong Kong: Law prohibiting the transfer of personal data soon to come into Force, 16 Jan. Available at http://www.twobirds.com.

Cobb, S. (2016), Data privacy and data protection: US law and legislation, *An ESET White Paper*, 1-15. Available at http://www.welivesecurity.com.

Council of Europe (2014), Handbook on European data protection law. Available at http://fra.europa.eu.

Culnan, M. (2002). Georgetown Internet Privacy Policy Study. McDonough School of Business, Georgetown University, see http://www.msb.edu/faculty/culnan/gippshome.html.

European Organization for Security (EOS)-Privacy & Data Protection Task Force (2010). EU policies on privacy and data protection and their impact on the implementation of security solutions. Sept., 1-17.

European Commission (2011). Workshop on Privacy protection and ICT: Research ideas. *Workshop Report*, Sept.21, Brussels.

European Commission & Union (1998), Directive on Data Protection (Directive 95), available at http://eur-lex.europa.eu.

E&Y (2014) Privacy Trends 2014: Privacy Protection in the age of Technology. Available at www.ey.com. 1-24.

Federal Trade Commission (2010). Protecting Consumer Privacy in an Era of Rapid Change: A proposed framework for business and policymakers. December. Available at www.ftc.org.

Fuchs, C. (2011). The political economy of privacy on Facebook. *The Internet & Surveillance*, Research paper 9 series, Vienna, Australia. Available at www.uti.at.

Geller, T. (2016). In Privacy Law, It is the U.S. vs. the World, *Communications of the ACM*, 59(2), 21-23.

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science*, 57(1), 57-71.

Greenleaf, G. (2015b). Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, *33 Privacy Laws & Business International Report*, February, *UNSW Law Research Paper* No. 2015-21.

Greenleaf, G. (2015). Hong Kong data privacy 2015: Cautious enforcement, strong principles, *Privacy Laws & Business International Report*, 21-23, December, 1-5.
Greenleaf, G. (2015a). Confusion as Indian Supreme Court Compromises on Data Privacy and ID Number, 28 Sept. Privacy Laws & Business International Report, 24-26, Sept. UNSW Law Research Paper No. 2016-06. Available at http://papers.ssrn.com.
Internet Policy Task Force Report (2010), Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Department of Commerce and Internet Policy Task Force Report. Available at http://www.ntia.doc.gov/
Kolekar, Y.P. (2015), Protection of Data under Information Technology Law in India, 27 April, 1-12. Available at SSRN: http://ssrn.com/abstract=2599493.
Krill, P. (2002). DoubleClick Discontinues Web Tracking Service. *InfoWorld*, 9 January. Available at: http://www.infoworld.com/articles.
Kugler, L. (2015). Online Privacy: Regional Differences, *Communications of the ACM*, Feb., 58(2), 18-20.
Laudon, K.C & Traver, C.G. (2014). E-commerce 10th edition, Addison Wesley, NY.
Laudon, K.C. and Laudon, J.P. (2016) Management Information Systems: Managing the digital firm. Pearson, 14th edition.
Majid, A. (2016), Malaysia: Personal Data Protection Standards - 12 Jan. Available at http://www.mondaq.com.
Mantelero, A. (2012), Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution', *European Journal for Law and Technology*, 3(2).
Morando, F., Iemma, R., & Raiteri, R. (2014). Privacy evaluation: what empirical research on users' valuation of personal data tells us, *Internet Policy Review*, 3(2), May, available at http://policyreview.info.
Office of the Privacy Commissioner of Canada (2016). The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments, available at https://www.priv.gc.ca.
Organization for Economic Co-operation and Development (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at http://www.oecd.org.
Parsons, M. and Colegate, P. (2015), The Turning Point for Data Privacy Regulation in Asia? *Chronicle of Data Protection*, 18 Feb. Available at http://www.hldataprotection.com.
Pfeifle, S. (2015), The Regulators' View of the Singapore Privacy Law, *The Privacy Advisor*, 12 May, available at https://iapp.org.
Pierce, L. (2013), Protection of Personal Information Act: Are you compliant? *Mail & Guardian*, Dec. 2. Available at http://mg.co.za/article/2013-12-02-protection-of-personal-information-act-are-you-compliant.
Robert, J. (2011), Five Solutions To The Privacy Problem: Why They Work And Why They Don't. Available at https://gigaom.com.
Sotto, L.J. and Hydak, C.D. (2016), The EU-US Privacy Shield: A How-To Guide, *Law360*, July 19, 1-4.
Srinivas, B.V. (2015), A Concise Guide to Various Australian Laws Related to Privacy and Cyber Security Domains, *SANS Institute InfoSec Reading Room Site*, 1-30. Available at https://www.sans.org.
Srivas, A. (2016), Cross-Border Data Flows Debate Hits India as TRAI Issues Paper on Cloud Services, *The Wire*, 11 June, available at http://thewire.in.
Shah, A. and Zacharias, N. (2010), Right to privacy and data protection, Nitin Desai Associates, Mumbai.
Slyke, C.V., & Belanger, F. (2012). E-Business Technologies: Supporting the Net-Enhanced Organization. John Wiley & Sons.
Stevens, Toby (2016), Data Protection: Objectives or Outcomes? 14 Sept. Available at ComputerWeekly.com.
Stevens, G. (2011). Privacy protections for personal information online, April, Congressional Research Service Report 7-5700, available at www.crs.gov.
Swire, P., Hemmings, J. & Kirkland, A. (2016). Online Privacy and ISPS, working paper of The Institute for Information Security & Privacy, Feb. 29. Available at http://www.iisp.gatech.edu.
Thiel, S. and Biggs, C. (2016), Singapore's enforcement of data protection law on the rise, 23 Aug. DLA Piper, available at https://www.technologyslegaledge.com.
Thiel, S. and Biggs, C. (2016a), Hong Kong's Privacy Commissioner addresses privacy compliance and best practice for BYOD, 21 Sept. available at http://blogs.dlapiper.com.
UNESCO (2012). Preserving Privacy in the Information Society. Available at electronically at www.unesco.org.
Weiss, M.A. & Archick, K. (2016), U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research Service, 7-5700. 1-16. Available at www.crs.gov.
Wirtz, J., Lewin, M.O. & Williams, J.D. (2007). Causes and Consequences of consumer online privacy concern. *International Journal of Service Industry Management*, 18(4), 326-348.
World Privacy Forum Report (2011), Many Failures: A Brief History of Privacy Self-Regulation. 14 Oct. Available at https://www.worldprivacyforum.org.
Yadav, Y. (2015), Centre Giving Final Touches to Right to Privacy Bill, 17 March, *Indian Express*, New Delhi.